

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

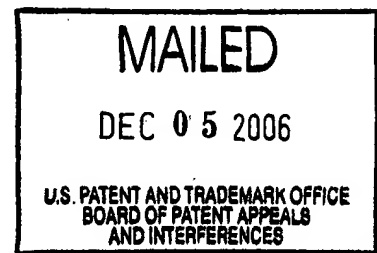
UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN MICHAEL EVERSON
AND JAMES W. NORRIS

Appeal No. 2006-3281
Application No. 09/664,893

ON BRIEF



Before HAIRSTON, HOMERE, and LUCAS, Administrative Patent Judges.

HAIRSTON, Administrative Patent Judge.

DECISION ON APPEAL

This is an appeal from the final rejection of claims 1 through 12 and 21 through 36.

The disclosed invention relates to a method and system for authenticating and authorizing a computer user to a plurality of separately secured remote applications via use of an object stored in a directory of a directory server. The object contains security information relating to the computer user, and a link to the object is stored on the user's computer during the launching of a first application. When the computer user launches a second application, the link to the object between the user's computer and the directory server is used to authenticate and authorize the computer user's access to the second application.

Claim 32 is illustrative of the claimed invention, and it reads as follows:

32. A system for authenticating and authorizing a user remotely launching secured computer applications from a user computer, the system comprising:

an authorization server for authenticating and authorizing the user to the secured computer applications by exchanging security information between the user and the authorization server when a first secured computer application is launched by the user;

a directory server storing at least a portion of the security information in an object within a dynamic directory, wherein a link to the object is stored on the user computer; and

an application server implementing a second separately-secured computer application for remote launching by the user, wherein the second separately-secured computer application retrieves the link, and wherein the user is authenticated and authorized to the second separately-secured computer application by exchanging the stored security information between the directory server and the application server.

The references relied on by the examiner are:

Hartman et al. (Hartman)	5,960,411	Sept. 28, 1999
Alegre et al. (Alegre)	6,199,113	Mar. 6, 2001 (filed Apr. 15, 1998)
Blanco et al. (Blanco)	6,539,482	Mar. 25, 2003 (filed Apr. 8, 1999)

Claims 1 through 4, 7 through 10, 21, 24, 27, 29, 30, 32, 34 and 35 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Alegre.

Claims 5, 6, 11, 12, 31 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Alegre in view of Hartman.

Claims 22, 23, 25, 26, 28 and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Alegre in view of Blanco.

Reference is made to the briefs and the answer for the respective positions of the appellants and the examiner.

OPINION

We have carefully considered the entire record before us, and we will reverse the anticipation rejection of claims 1 through 4, 7 through 10, 21, 24, 27, 29, 30, 32, 34 and 35, and reverse the obviousness rejections of claims 5, 6, 11, 12, 22, 23, 25, 26, 28, 31, 33 and 36.

Anticipation is established when a single prior reference discloses, expressly or under the principles of inherency, each and every element of a claimed invention as well as disclosing structure which is capable of performing the recited functional limitations. RCA Corp. v. Applied Digital Data Systems, Inc., 730 F.2d 1440, 1444, 221 USPQ 385, 388 (Fed. Cir. 1983).

Turning first to the anticipation rejection, we find that all of the claims on appeal include an object stored in a directory server during the use of a first application, and a link between the object stored in the directory server and information stored on the user's computer to gain authentication and authorization to use a second application.

During a log-in operation in Alegre, web host 210 requests user authentication information from the computer user at client browser 110 (Figure 2; column 4, lines 24 through 26). Upon receiving the information from the user, the web host 210 requests authentication of the information from authentication server 226 (column 4, lines 26 through 30). If the user information is valid, then the authentication server 226 receives a user access profile from

authentication database 224 (column 4, lines 31 through 35). Thereafter, authentication server 226 requests a session key from key server 234 (column 4, lines 35 and 36). The key server stores the unique session key along with the information provided by the user in key database 236 (column 4, lines 36 through 40). The authorization server 226 then transmits the session key and user access profile to the web host 210 (column 4, lines 40 and 41). The web host 210 stores the session key at client browser 110 using a cookie (column 4, lines 41 and 42). The web host 210 also sends trusted network access presentation information that the user will need to use to access the trusted network 138 (column 4, lines 42 through 47). When access to the trusted network 138 is needed, the user selects an access request from the trusted network access presentation information (e.g., a URL associated with the selection) and sends the request along with the session key to the web host 210 where it is processed and placed into a network request packet prior to transmission to access server 222 (column 4, lines 48 through 54). The access server 222 verifies that the request packet came from the web host 210, extracts the session key from the request packet and transfers the session key to key server 234 to determine the validity of the session key (column 4, lines 55 through 58). If the session key is valid, the key server 234 notification to the access server 222 permits the access server to perform the request (column 4, lines 58 through 63).

During a next request, a new session key is needed to gain access to the trusted network 138 (column 6, lines 23 through 67).

Appeal No. 2006-3281
Application No. 09/664,893

Appellants argue (brief, pages 8 and 9) that Alegre “requires every message transmitted from the user to the network to be authenticated,” lacks a teaching of “using a directory to store an object accessed by more than one application for purposes of authentication,” and lacks a teaching of “a second application accessing an object created when an earlier application was launched.” We agree with appellants’ arguments. We additionally agree with the appellants’ argument (reply brief, page 2) that the session key and cookie in Alegre are not objects that are stored and used in the manner set forth in the claims on appeal. Even if we assume for the sake of argument that a session key and cookie can be objects, Alegre lacks a directory server that stores the objects and provides a link to the user’s computer as required by all of the claims on appeal.

In summary, the anticipation rejection of claims 1 through 4, 7 through 10, 21, 24, 27, 29, 30, 32, 34 and 35 is reversed.

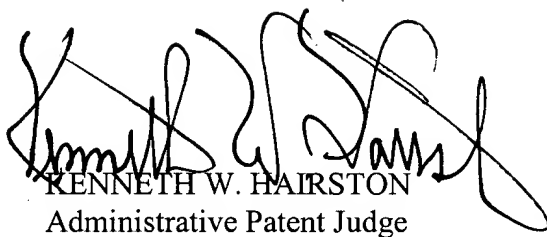
The obviousness rejections of claims 5, 6, 11, 12, 22, 23, 25, 26, 28, 31, 33 and 36 are reversed because the teachings of Hartman and Blanco fail to cure the noted shortcomings in the teachings of Alegre.

DECISION

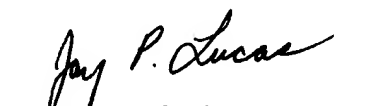
The decision of the examiner rejecting claims 1 through 4, 7 through 10, 21, 24, 27, 29, 30, 32, 34 and 35 under 35 U.S.C. § 102(e) is reversed, and the decision of the examiner rejecting claims 5, 6, 11, 12, 22, 23, 25, 26, 28, 31, 33 and 36 under 35 U.S.C. § 103(a) is reversed.

Appeal No. 2006-3281
Application No. 09/664,893

REVERSED


KENNETH W. HAIRSTON
Administrative Patent Judge


JEAN R. HOMERE
Administrative Patent Judge


JAY P. LUCAS
Administrative Patent Judge

)
)
)
)
)
) BOARD OF PATENT
) APPEALS
) AND
) INTERFERENCES
)
)
)
)
)

KWH/kis

Appeal No. 2006-3281
Application No. 09/664,893

SPRINT COMMUNICATIONS COMPANY, L.P.
6391 SPRINT PARKWAY
MAILSTOP: KSOPHT0101-Z2100
OVERLAND PARK, KS 66251-2100